

03500.015945



PATENT APPLICATION 44

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
Satoru WAKAO, et al.) Examiner: Not Assigned
Application No.: 09/987,832) Group Art Unit: 2612
Filed: November 16, 2001)
For: IMAGE DATA VERIFICATION SYSTEM) January 28, 2002

The Commissioner for Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENTS

Sir:

In support of Applicants' claim for priority under 35 U.S.C. § 119, enclosed are
certified copies of the following Japanese applications:

2000-351529, filed November 17, 2000; and 2001-346689, filed November 12, 2001.

Applicants' undersigned attorney may be reached in our Washington office by
telephone at (202) 530-1010. All correspondence should continue to be directed to our address
given below.

Respectfully submitted,

Attorney for Applicants
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/cm

DC_MAIN 65321 v 1



CFO 15945 US / hda
09/987,832
Satoru Wajima, et al
11/16/01

日本特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年11月17日

出願番号

Application Number:

特願2000-351529

出願人
Applicant(s):

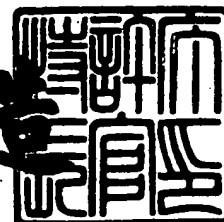
キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年12月 7日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3107157

【書類名】 特許願

【整理番号】 4253001

【提出日】 平成12年11月17日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 検証データ変換装置、ディジタルデータ改竄検出システム、検証データ変換方法、ディジタルデータ改竄検出方法、データ検証システム及び記録媒体

【請求項の数】 35

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

【氏名】 若尾 聡

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

【氏名】 岩村 恵市

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100090273

【弁理士】

【氏名又は名称】 國分 孝悦

【電話番号】 03-3590-8901

【手数料の表示】

【予納台帳番号】 035493

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 検証データ変換装置、デジタルデータ改竄検出システム、検証データ変換方法、デジタルデータ改竄検出方法、データ検証システム及び記録媒体

【特許請求の範囲】

【請求項 1】 外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、

秘密情報を用いて該映像データから 2 次検証データを生成する検証データ生成部とを有する検証データ変換装置。

【請求項 2】 上記請求項 1 において、共有情報と秘密情報を格納する記憶部を有することを特徴とする検証データ変換装置。

【請求項 3】 上記請求項 1 又は 2 において、映像データが改竄されていないかどうかを検証する時に、ハッシュ関数を用いることを特徴とする検証データ変換装置。

【請求項 4】 上記請求項 1 ～ 3 のいずれか 1 項において、秘密情報は公開鍵暗号方式の秘密鍵であることを特徴とする検証データ変換装置。

【請求項 5】 上記請求項 1 ～ 4 のいずれか 1 項において、公開鍵暗号方式の秘密鍵と公開鍵のペアを生成することを特徴とする検証データ変換装置。

【請求項 6】 上記請求項 1 ～ 5 のいずれか 1 項において、映像データ、2 次検証データ、及び公開鍵を出力する出力部を有することを特徴とする検証データ変換装置。

【請求項 7】 共有情報を用いて該映像データに対する検証データを生成する検証データ生成部と、映像データと検証データとを少なくとも記憶するデータ記憶部と、該映像データと検証データを出力する出力部とを有する映像入力装置と、

映像入力装置からの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて 2 次検証データを生成する検証データ生成部とを有する検証データ変換装置と、

検証データ変換装置で生成された２次検証データと、検証データ変換装置で用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する映像検証装置とを有することを特徴とするデジタルデータ改竄検出システム。

【請求項 8】 上記請求項 7 において、映像入力装置は、共有情報を記憶する記憶部を有することを特徴とするデジタルデータ改竄検出システム。

【請求項 9】 上記請求項 7 又は 8 において、映像入力装置は、映像を撮影する撮像部を有することを特徴とするデジタルデータ改竄検出システム。

【請求項 10】 上記請求項 7～9 のいずれか 1 項において、映像入力装置は、検証データを生成する時に、ハッシュ関数を用いることを特徴とするデジタルデータ改竄検出システム。

【請求項 11】 上記請求項 7～10 のいずれか 1 項において、映像入力装置は、撮像した映像データと生成した検証データとを外部に出力する出力部を有することを特徴とするデジタルデータ改竄検出システム。

【請求項 12】 上記請求項 7～11 のいずれか 1 項において、映像検証装置は、公開情報を外部から入力するための入力部を有することを特徴とするデジタルデータ改竄検出システム。

【請求項 13】 上記請求項 7～12 のいずれか 1 項において、映像検証装置で用いられる公開情報は、公開鍵暗号方式の公開鍵であることを特徴とするデジタルデータ改竄検出システム。

【請求項 14】 上記請求項 7～13 のいずれか 1 項において、映像入力装置と検証データ変換装置がインタフェース部をそれぞれ有し、一体の装置として動作することを特徴とするデジタルデータ改竄検出システム。

【請求項 15】 上記請求項 7～14 のいずれか 1 項において、検証データ変換装置は、外部装置とのインタフェース部とデータ記憶部とデータ演算部とを少なくとも有することを特徴とするデジタルデータ改竄検出システム。

【請求項 16】 上記請求項 7～15 のいずれか 1 項において、検証データ変換装置は、ICカードであることを特徴とするデジタルデータ改竄検出システム。

【請求項 1 7】 外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、

秘密情報を用いて該映像データから 2 次検証データを生成する検証データ生成ステップとを有する検証データ変換方法。

【請求項 1 8】 上記請求項 1 7 において、共有情報と秘密情報を格納する記憶ステップを有することを特徴とする検証データ変換方法。

【請求項 1 9】 上記請求項 1 7 又は 1 8 において、映像データが改竄されていないかどうかを検証する時に、ハッシュ関数を用いる演算ステップを有することを特徴とする検証データ変換方法。

【請求項 2 0】 上記請求項 1 7 ～ 1 9 のいずれか 1 項において、公開鍵暗号方式の秘密鍵と公開鍵のペアを生成するステップを有することを特徴とする検証データ変換方法。

【請求項 2 1】 上記請求項 1 7 ～ 2 0 のいずれか 1 項において、映像データ、2 次検証データ、及び公開鍵を出力する出力ステップを有することを特徴とする検証データ変換方法。

【請求項 2 2】 共有情報を用いて該映像データに対する検証データを生成する検証データ生成ステップと、映像データと検証データとを少なくとも記憶するデータ記憶ステップと、該映像データと検証データを出力する出力ステップとを有する映像入力ステップと、

映像入力ステップからの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて 2 次検証データを生成する検証データ生成ステップとを有する検証データ変換ステップと、

検証データ変換ステップで生成された 2 次検証データと、検証データ変換ステップで使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する検証ステップを有する映像検証ステップとを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 2 3】 上記請求項 2 2 において、映像入力ステップは、共有情報

を記憶する記憶ステップを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 24】 上記請求項 22 又は 23 において、映像入力ステップは、映像を撮影する撮像ステップを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 25】 上記請求項 22～24 のいずれか 1 項において、映像入力ステップは、検証データを生成する時に、ハッシュ関数を用いる演算ステップを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 26】 上記請求項 22～25 のいずれか 1 項において、映像入力ステップは、撮像した映像データと生成した検証データとを外部に出力する出力ステップを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 27】 上記請求項 22～26 のいずれか 1 項において、映像検証ステップは、公開情報を外部から入力するための入力ステップを有することを特徴とするデジタルデータ改竄検出方法。

【請求項 28】 上記請求項 22～27 のいずれか 1 項において、映像検証ステップで用いられる公開情報は、公開鍵暗号方式の公開鍵であることを特徴とするデジタルデータ改竄検出方法。

【請求項 29】 請求項 17～28 のいずれか 1 項に記載のステップをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 30】 計算能力に応じて、映像データから演算処理負荷の少ない 1 次検証データを生成する 1 次検証データ生成装置と、

該 1 次検証データを検証後、映像データから演算処理負荷の大きい 2 次検証データを生成する 2 次検証データ生成装置と、

映像データと該 2 次検証データとを用いて該映像データの改竄検出を行う検証装置とを有することを特徴とするデータ検証システム。

【請求項 31】 上記請求項 30 において、1 次検証データ生成時と 1 次検証データ検証時に共有情報を用いることを特徴とするデータ検証システム。

【請求項 32】 上記請求項 30 又は 31 において、2 次検証データ生成時

に秘密情報を用いることを特徴とするデータ検証システム。

【請求項 3 3】 上記請求項 3 0 ～ 3 2 のいずれか 1 項において、2 次検証データ検証時に公開情報を用いることを特徴とするデータ検証システム。

【請求項 3 4】 上記請求項 3 2 又は 3 3 において、秘密情報は、公開鍵暗号方式の秘密鍵であり、公開情報は公開鍵暗号方式の公開鍵であることを特徴とするデータ検証システム。

【請求項 3 5】 上記請求項 3 0 ～ 3 4 のいずれか 1 項において、1 次検証データ生成、検証時および 2 次検証データ生成、検証時にハッシュ関数を用いることを特徴とするデータ検証システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、撮影対象の映像情報をデジタルデータに変換し、改竄検出用データをデジタルデータに付加することで該映像情報の改竄を検出する技術に関する。

【0 0 0 2】

【従来の技術】

近年、従来の銀塩写真や 8mm フィルムに替わって、撮影した情報をデジタル化し、デジタルデータとして記録媒体等に記録するデジタルカメラといった映像入力装置が実用化されている。これにより、撮影した情報そのものをパーソナルコンピュータを始めとする情報処理装置に移し、表示させることが可能になった。このような映像データを通信回線を利用することで全国どこでも瞬時に映像データを送信することも可能になった。そのため、事故処理で証拠写真を扱う保険会社や建築現場の進捗状況の記録を扱う建設会社においてデジタル映像データの利用が考えられている。

【0 0 0 3】

しかし一方で目覚ましいデータ処理技術の進歩により、映像データを始めとしたデジタルデータの編集をフォトタッチツールや動画編集ツール等の使用で容易に行うことが可能になった。そのため、デジタル映像データの信頼性は従来

の銀塩写真等と比較して低く、証拠としての能力に乏しいという問題があった。そこで映像データの改ざん、偽造が行われていた場合にそれを検出するような映像入力装置、システムが提案されてきた。

【0004】

例えば”DIGITAL CAMERA WITH APPARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE ”という名称の米国特許第5499294や”映像入力装置および映像入力システム”という名称の特許出願公開番号：特開平9-200730 によると映像入力装置に固有の秘密情報および該映像入力装置に接続される外部装置に固有の秘密情報の少なくとも一方の情報と該映像入力装置にて撮影してデジタル化したデジタルデータとに基づき、所定の演算を実行して該デジタルデータを識別する情報、すなわちデジタル署名データを生成し、該デジタル署名データと映像入力装置にて撮影してデジタル化したデジタルデータとを映像入力装置の出力とするものである。また、上記公報ではデジタル署名データ生成にハッシュ関数と公開鍵暗号を使用している。公開鍵暗号については後で説明する。

【0005】

デジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することである。

【0006】

デジタル署名データ生成にハッシュ関数と公開鍵暗号を用いたデータの正当性の確認は以下のようになり、これが上記公報の方法である。

【0007】

秘密鍵を K_s 、公開鍵を K_p とすると発信者は、平文データ M をハッシュ関数により圧縮して一定長の出力 h を算出する演算を行う。次に秘密鍵 K_s で h を変換してデジタル署名データ s を作成する演算すなわち $D(K_s, h) = s$ を行う。その後、該デジタル署名データ s と平文データ M とを送信する。一方受信者は受信したデジタル署名データ s を公開鍵 K_p で変換する演算すなわち $E(K_p, s) = E(K_p, D(K_s, h')) = h'$ と、受信した平文データ M' を発信者と同じハッシュ関数により圧

縮して h' を算出する演算を行い、 h' と h'' が一致すれば受信したデータ M' を正当であると判断する。

【0008】

平文データ M が送受信間で改ざんされた場合には $E(Kp, s) = E(Kp, D(Ks, h'')) = h'$ と、受信した平文データ M' を発信者と同じハッシュ関数により圧縮した h' が一致しないので改ざんを検出できる。ここで、平文データ M の改ざんに合わせてデジタル署名データ s の改ざんも行われてしまうと改ざんの検出ができなくなる。しかし、これは h から平文データ M を求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。

【0009】

次にハッシュ関数について説明する。ハッシュ関数は上記デジタル署名の生成を高速化するため等に用いられる。ハッシュ関数は任意の長さの平文データ M に処理を行い、一定の長さの出力 h を出す機能を持つ。ここで、出力 h を平文データ M のハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とは h を与えた時、 $h=H(M)$ となる平文データ M の算出が計算量的に困難であることである。衝突耐性とは平文データ M を与えた時、 $H(M)=H(M')$ となる平文データ M' ($M \neq M'$)の算出が計算量的に困難であること及び $H(M)=H(M')$ かつ $M \neq M'$ となる平文データ M, M' の算出が計算量的に困難であることである。

【0010】

ハッシュ関数としてはMD-2, MD-4, MD-5, SHA-1, RIPEMD-128, RIPEMD-160等が知られており、これらのアルゴリズムは一般に公開されている。

【0011】

続いて公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の特徴としては、

(a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密

に記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。
が挙げられる。

【 0 0 1 2 】

例えば、平文データ M に対して、公開の暗号鍵 K_p を用いた暗号化操作を $E(K_p, M)$ とし、秘密の復号鍵 K_s を用いた復号操作を $D(K_s, M)$ とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

【 0 0 1 3 】

(1) K_p が与えられたとき、 $E(K_p, M)$ の計算は容易である。 K_s が与えられたとき、 $D(K_s, M)$ の計算は容易である。

(2) もし K_s を知らないなら、 K_p と E の計算手順と $C = E(K_p, M)$ を知っていても、 M を決定することは計算量の点で困難である。

【 0 0 1 4 】

次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

(3) 全ての平文データ M に対し、 $E(K_p, M)$ が定義でき、 $D(K_s, E(K_p, M)) = M$ が成立する。つまり、 K_p は公開されているため誰もが $E(K_p, M)$ を計算することができるが、 $D(K_s, E(K_p, M))$ を計算して M を得ることができるのは秘密鍵 K_s を持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

【 0 0 1 5 】

(4) すべての平文データ M に対し、 $D(K_s, M)$ が定義でき、 $E(K_p, D(K_s, M)) = M$ が成立する。つまり、 $D(K_s, M)$ を計算できるのは秘密鍵 K_s を持っている本人のみであり、他の人が偽の秘密鍵 K_s' を用いて $D(K_s', M)$ を計算し K_s を持っている本人になりすましたとしても、 $E(K_p, D(K_s', M)) \neq M$ なので受信者は受けとった情報が不正なものであることを確認できる。また、 $D(K_s, M)$ が改ざんされても $E(K_p, D(K_s, M)') \neq M$ となり、受信者は受けとった情報が不正なものであることを確認できる。

【 0 0 1 6 】

上記の秘密通信と認証通信とを行うことができる代表例としてRSA暗号やR暗号やW暗号等が知られている。

【 0 0 1 7 】

ここで、現在最も使用されているRSA暗号の暗号化、復号は次式で示される。

暗号化：暗号化鍵 (e, n) 暗号化変換 $C = M^e \pmod{n}$

復号：復号鍵 (d, n) 復号変換 $M = C^d \pmod{n}$

$n = p \cdot q$ ここで p, q は大きな異なる素数

【 0 0 1 8 】

上記のように、RSA暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、DESをはじめとする共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。

【 0 0 1 9 】

【発明が解決しようとする課題】

しかし、該公開鍵暗号を用いたデジタル署名データ生成を該映像入力装置で行う場合、処理時間がかかるか、処理時間を速くする場合には、映像入力装置のCPU（中央演算処理装置）、メモリ（記録媒体）といったハードウェア上の能力を向上させる必要がある。しかしこの向上は結果として製品のコストアップの要因となり好ましくない。

【 0 0 2 0 】

これは、映像入力装置の演算リソース（CPU（中央演算処理装置）、メモリ（記録媒体））は映像データの撮影時の処理等のみに使用されることを前提に設計されているものであるため、これらのリソースをデジタル署名データ生成の処理に振り分ける余地が少ないこと、及び公開鍵暗号方式は共通鍵暗号方式に比較して多く計算を必要とするためによるものである。

【 0 0 2 1 】

代表的な公開鍵暗号方式として前述のRSAがあるが、前に記述したようにこの方式はべき乗演算と剰余演算が必要であるために演算処理が複雑となり、DESをはじめとする共通鍵暗号方式の数百倍から数千倍の処理時間が必要であるとされ

ている。従って、豊富な演算リソースを有しない映像入力装置で撮影した映像データの完全性（データの改竄が行われていないこと）を保証するためのデータをいかにして生成するかという問題がある。

【0022】

また、上記にて生成した完全性を保証するためのデータを基にして何処の装置で、何時、どのように検証を行うかといった、検証システム全体をどのように構築するのかといった問題もある。さらには、該完全性を保証するために生成されたデータを用いて、映像データの完全性を検証する時に必要となる情報の存在場所の明示方法や映像データをどのように管理すれば効率的に管理ができるかといった問題がある。

【0023】

本発明の目的は、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することであり、さらには、該映像データに関するデータを（映像データと）関連付けることでデータベースを作成して管理等を容易にし、トータルな映像データの認証システムを構築することである。

【0024】

【課題を解決するための手段】

本発明の一観点によれば、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて該映像データから2次検証データを生成する検証データ生成部とを有する検証データ変換装置が提供される。

【0025】

本発明の他の観点によれば、共有情報を用いて該映像データに対する検証データを生成する検証データ生成部と、映像データと検証データとを少なくとも記憶するデータ記憶部と、該映像データと検証データを出力する出力部とを有する映像入力装置と、映像入力装置からの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて

2次検証データを生成する検証データ生成部とを有する検証データ変換装置と、検証データ変換装置で生成された2次検証データと、検証データ変換装置で使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する映像検証装置とを有することを特徴とするデジタルデータ改竄検出システムが提供される。

【0026】

本発明のさらに他の観点によれば、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて該映像データから2次検証データを生成する検証データ生成ステップとを有する検証データ変換方法が提供される。

【0027】

本発明のさらに他の観点によれば、共有情報を用いて該映像データに対する検証データを生成する検証データ生成ステップと、映像データと検証データとを少なくとも記憶するデータ記憶ステップと、該映像データと検証データを出力する出力ステップとを有する映像入力ステップと、映像入力ステップからの映像データと検証データとに基づいて該映像データが改竄されていないかどうかを検証する検証処理ステップと、秘密情報を用いて2次検証データを生成する検証データ生成ステップとを有する検証データ変換ステップと、検証データ変換ステップで生成された2次検証データと、検証データ変換ステップで使用された秘密情報に対応する公開情報とに基づいて該映像データの改竄を検証する検証ステップを有する映像検証ステップとを有することを特徴とするデジタルデータ改竄検出方法が提供される。

【0028】

本発明のさらに他の観点によれば、計算能力に応じて、映像データから演算処理負荷の少ない1次検証データを生成する1次検証データ生成装置と、該1次検証データを検証後、映像データから演算処理負荷の大きい2次検証データを生成する2次検証データ生成装置と、映像データと該2次検証データとを用いて該映像データの改竄検出を行う検証装置とを有することを特徴とするデータ検証シス

テムが提供される。

【 0 0 2 9 】

本発明によれば、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することができる。

【 0 0 3 0 】

【発明の実施の形態】

以下、本発明の実施形態を、実施例に沿って図面を参照しながら説明する。

映像データの改竄を検出するためのシステムを構成する映像入力装置、検証データ変換装置、映像検証装置の構成について図 1 ～ 3 に基づいて説明し、次に映像データの改竄検出システムにおける装置間の処理に関して図 4 に基づいて説明し、続いて各装置の処理フローに関して図 9 ～ 1 1 に基づいて説明する。

【 0 0 3 1 】

映像入力装置の構成

図 1 は、本発明における実施例の映像入力装置の構成を示す図であり、図における各ブロックは機能別の構成要素である。制御/演算部 1 1 は撮影指示がなされると、ROM 1 7 にあらかじめ格納されているプログラムに従い映像データの圧縮処理、検証データ生成等の各種演算処理を行う。駆動部 1 2 は撮影に必要な機械的な動作を制御/演算部 1 1 の制御のもとで行う。作業用メモリ 1 3 では映像データが一時的に保管され、ここで該映像データの圧縮及び各種演算処理が行われる。

【 0 0 3 2 】

光学系 1 4 は電荷結合素子 CCD または光学センサーを含み、撮影指示がなされると被写体の撮影、電気信号処理、ディジタル信号処理等を行う。保管用メモリ 1 5 は処理済の映像データを格納する。

【 0 0 3 3 】

外部装置とのインタフェース部 1 6 はメモリカード、携帯端末、通信装置といった外部装置とのインタフェースであり、映像データや検証データをこれらの機器へ送信する時に使用される。

【 0 0 3 4 】

ROM 1 7 は読み出し専用メモリであり、あらかじめ動作プログラムや検証データ生成に必要な共有情報が格納される。操作部 1 8 は撮影者の撮影指示をはじめとする各種の指示を受け付けるためのものである。

【 0 0 3 5 】

検証データ変換装置の構成

図 2 は、本発明における実施例の検証データ生成装置の構成を示す図であり、図における各ブロックは機能別の構成要素である。

【 0 0 3 6 】

インタフェース部 2 4 は映像入力装置、映像検証装置といった外部装置とのインタフェースであり、検証データが挿入された映像データや該映像データの検証に必要な共有情報や、2 次検証データ生成に必要な秘密情報を受信する時、さらには、2 次検証データが挿入された映像データを送信する時に使用され、受信した映像データや共有情報は保管用メモリ 2 5 に、格納される。

【 0 0 3 7 】

入力された映像データの検証指示が操作部 2 7 に対してなされると、ROM 2 6 にあらかじめ格納されているプログラムに従い検証データの検証処理を作業用メモリ 2 3 にて行う。該検証処理に必要な共有情報はあらかじめ ROM 2 6 に格納されていて必要時に ROM 2 6 から作業用メモリ 2 3 に読み込まれるか、外部インタフェース部 2 4 を通して外部の装置から作業用メモリ 2 3 に読み込まれる。検証の結果、映像データの改竄が為されていないと判断した場合には引き続いて 2 次検証データ生成が映像データと保管用メモリ 2 5 に格納されている秘密情報とを用いて行われる。該秘密情報は、あらかじめ保管用メモリ 2 5 に格納されているか、制御/演算部 2 1 の指示により作業用メモリ 2 3 にて生成された後に保管用メモリ 2 5 に格納されるか、さらには、外部装置から受信して保管用メモリ 2 5 に格納される。

【 0 0 3 8 】

ROM 2 6 は読み出し専用メモリであり、あらかじめ検証プログラム、2 次検証データ生成プログラムが格納される。操作/入力部 2 7 は起動指示、検証指示を

はじめとするユーザからの各種指示を受け付けるためのものである。

【 0 0 3 9 】

作業用メモリ 2 3 では受信した映像データが保管用メモリ 2 5 から移され、ここで該映像データの検証処理、2 次検証データ生成及び各種演算処理が行われる。出力部 2 2 は、検証処理結果をディスプレイやプリンタといった外部の装置に出力する。

【 0 0 4 0 】

映像検証装置の構成

図 3 は、本発明における実施例の映像検証装置の構成を示す図であり、図に示される各ブロックは機能別の構成要素である。

【 0 0 4 1 】

インタフェース部 3 4 は映像データ検証装置といった外部装置とのインタフェースであり、映像データや、映像データの検証に必要なとなる秘密情報に対応する公開情報を受信する時に使用される。

【 0 0 4 2 】

入力された映像データの検証指示が操作部 3 7 に対してなされると、ROM 3 6 にあらかじめ格納されているプログラムに従って、制御／演算部 3 1 が映像データに付加されている検証データの検証処理を作業用メモリ 3 3 にて行う。該検証処理に必要なとなる公開情報はあらかじめROM 3 6 に格納されていて必要時にROM 3 6 から作業用メモリ 3 3 に読み込まれるか、外部インタフェース部 3 4 を通して外部の装置から作業用メモリ 3 3 に読み込まれる。

【 0 0 4 3 】

ROM 3 6 は読み出し専用メモリであり、あらかじめ検証プログラムが格納される。操作／入力部 3 7 は起動指示、検証指示をはじめとするユーザからの各種指示を受け付けるためのものである。

【 0 0 4 4 】

作業用メモリ 3 3 では受信した映像データが保管用メモリ 3 5 から移され、ここで該映像データの検証処理及び各種演算処理が行われる。出力部 3 2 は、検証処理結果をディスプレイやプリンタといった外部の装置に出力する。

【 0 0 4 5 】

受信した映像データに対して、改竄の有無、改竄検出に必要となる公開情報の
 ありか、どの検証データ変換装置から送られてきたものか、登録日時、検証日時
 等の情報を関連付けてデータベースを作成し、保管用メモリ 3 5 に記憶する。

【 0 0 4 6 】

図 4 は、本実施例における、各装置の処理を示す図である。以下では図 4 中の
 (1) から (1 1) の番号と以下の (1) から (1 1) の番号とを対応させて説
 明する。映像入力装置における検証データ生成処理は、図 5 に示すように映像デ
 ータに対して、共有情報との排他的論理和演算といった簡易な演算を行った後、
 ハッシュ関数による演算を行い、その出力を検証データとする方式とする。該検
 証データは検証データ変換装置において該共有情報を用いて検証後、公開鍵暗号
 演算を用いて生成した 2 次検証データと差し替えられる。該 2 次検証データは、
 映像検証装置において、公開鍵暗号演算を用いて検証される。

【 0 0 4 7 】

(1) 映像入力装置で被写体を撮影すると撮影された映像データは、電気信号
 処理、デジタル信号処理等が行われる。上記処理後、映像圧縮処理が行われて
 からファイルフォーマット化される。代表的な映像圧縮方式としては、JPEG (静
 止画) 、 MPEG (動画) 等が有名であり、ファイルフォーマットとしては、JFIF, T
 IFF, GIFF (静止画) が有名である。映像圧縮処理後、該圧縮された映像データが
 ROM に格納されている共有情報を用いて処理が行われて検証データが生成される
 。該処理について図 6 を用いて説明する。

【 0 0 4 8 】

ここでは、映像入力装置の共有情報として例えば " 1 1 1 1 1 1 1 " を考える。これは
 、映像入力装置の装置外に公開されずかつ検証データ変換装置と共有できればど
 のようなものでよい。またこの共有情報は、容易に外部へ情報が漏れないように
 管理する。上記映像データの所定位置のバイトと、秘密情報である " 1 1 1 1 1 1 1 " と
 のビット毎の排他的論理和演算が行われて中間データとなる。ここで、所定位置
 のバイトとして最上位バイトとする。但し、この所定位置のバイトとしては任意
 の位置とすることもできる。さらに、中間データの生成の演算として映像データ

と共有情報のビット毎の排他的論理和演算としたが、演算出力がこれら2つのデータのみに基づいて生成され、高速に処理可能なものであればどのような演算でもよい。最後に、中間データを入力としてハッシュ関数の演算処理が行われる。該処理で出力される値が検証データとなる。ハッシュ関数としては、MD-5, SHA-1 が特に有名であり、MD-5のハッシュ値は128ビットであり、SHA-1は160ビットである。従って、ハッシュ関数としてMD-5を採用すれば検証データは128ビットとなり、SHA-1を採用すれば160ビットとなる。該処理で得られた検証データは映像データと共有情報に固有の情報となり、改ざん者は入力である映像データを改ざんしても共有情報を知らないので、該映像データに対応する検証データを得ることができない。これはハッシュ関数の一方向性により、得られたハッシュ値からその元のデータを知ることができない、すなわち共有情報を知ることができないことから保証されるためである。よって、秘密情報を知らない改ざん者は映像データの改ざんが不可能になる。該検証データは、秘密情報がROMから外部に流出しない限り安全であることは、上記にて説明した通りである。

【 0 0 4 9 】

(2) 生成された検証データは、ファイルフォーマット化された映像データのヘッダ部の部分に挿入される。一例としてJFIF方式にてフォーマット化された映像データのヘッダ部に挿入されるデータ構成例を図7に示す。挿入されるデータは、識別子エリア、長さエリア、検証データエリアで構成される。識別子エリアには、ここからヘッダ部が始まること示すデータ（マーカ）が記述され、長さエリアには、長さエリアと検証データエリアとの合計のデータ長がバイト単位で記述され、検証データエリアには、上記で生成された検証データが記述される。映像データを再生（表示）する時にはこのヘッダ部は読み飛ばされるので、データを挿入することで画質の劣化、画像の変化が発生することはない。

【 0 0 5 0 】

(3) 検証データが挿入された映像データは、外部装置とのインタフェース部においてデータ変換された後に送出される。外部装置がネットワークである場合には、そのプロトコルに応じたデータ変換が行われ、外部装置がフロッピーディスク、メモ리카ード等の記録デバイスである場合には、該デバイスにデータの記

録が行われる。

【0051】

(4) 映像データを受け取った検証データ変換装置は、最初に映像データのヘッダ部の検証データを抽出する。次に映像データからデジタル署名データを含むヘッダ部を削除し、ヘッダ部を削除した映像データから上記(1)と同様にして検証データを生成する。上記(1)においては、映像データに対して共有情報("11111111")との排他的論理和演算を行った後、ハッシュ関数による演算をおこなったので、ここでも同様の演算を行う。

【0052】

(5) 該演算結果と映像データのヘッダ部から抽出された検証データとを比較する。2つのデータが一致した場合には、映像入力装置から検証データ変換装置の間で改竄が行われていないと判断し、映像データの2次検証データ生成処理を行う。一致しない場合には、改竄が行われたと判断しその結果を出力する(2次検証データ生成処理は行わない)。

【0053】

(6) 上記の比較処理にて改竄が行われていないと判断した場合には、2次検証データ生成処理を行う。該生成処理は、図8に示すように映像データ(受け取った映像データからヘッダ部を削除したデータ)に対して、ハッシュ関数による演算を行いダイジェストデータを生成し、次に該ダイジェストデータに対して秘密情報を鍵とする公開鍵暗号演算を行い、その出力を2次検証データとするものである。ここで、使用した秘密情報は、あらかじめ検証データ変換装置に組み込んでおいてもいいし、検証データ変換装置内部で生成して保持してもよい。公開鍵暗号演算として例えばRSA演算を用いる場合には、秘密鍵と公開鍵は以下のよう生成される。

【0054】

まず、任意の相異なる2つの大きな素数 p, q を生成するとともにその積 $n = p \cdot q$ を計算する。次に、 $(p-1)$ と $(q-1)$ の最小公倍数 L を計算し、 L と互いに素で L より小さい任意の整数 e を生成する。最後に次式を満たす整数 d を計算する。 $ed = 1 \pmod{L}$ 。公開鍵を (e, n) とし秘密鍵を (d, n) とする。上記では、公開鍵暗号演

算としてRSA演算を用いる場合について説明したが、これに限るものではなく、公開鍵暗号演算が行えるようなものであればどのようなものでもよい。

【0055】

検証データ変換装置には、PCといった映像検証装置よりも計算リソースが豊富な機器を使用することで、演算負荷の大きい公開鍵暗号演算を高速に処理することが可能になる。

【0056】

(7) 生成された2次検証データは、(2)と同様に映像データのヘッダ部に挿入(検証データと差し替え)される。2次検証データが挿入された映像データは、(3)と同様に外部装置とのインタフェース部においてデータ変換された後に送出される。

【0057】

(8) 映像データを受け取った映像検証装置は、最初に映像データのヘッダ部の2次検証データを抽出する。次に抽出した2次検証データに対して、検証データ変換装置で使用された秘密情報に対応する公開情報を鍵とする公開鍵暗号演算を行いダイジェストデータを生成する。

【0058】

(9) 映像データから2次検証データを含むヘッダ部を削除し、ヘッダ部を削除した映像データから上記(6)と同様にしてハッシュ関数によりダイジェストデータを生成する

【0059】

(10) 上記(8)で生成したダイジェストデータと、上記(9)で生成したダイジェストデータとを比較して2つのデータが一致した場合には検証データ変換装置から映像検証装置の間で改竄が行われていないと判断し、その旨の表示を行う。一方で、一致しない場合には改竄が行われたと判断しその旨の表示を行う。

【0060】

(11) 検証データ変換装置からの映像データに対して、改竄の有無、改竄検出に必要な公開情報のありか、どの検証データ変換装置から送られてきたも

のか、登録日時、検証日時等の情報を関連付けてデータベースを作成する。このようなデータベースを作成することで、撮影された映像データの管理を行う。

【0061】

本実施例では、映像入力装置での検証データ生成の方式として、「映像データに対して、共有情報との排他的論理和演算を行った後ハッシュ関数による演算を行い、その出力を検証データとする」ものであったが、演算リソースの少ない装置でも現実的な時間で処理できる演算方法であれば、これに限るものではない。

【0062】

このように本方式は、映像入力装置において剰余算やべき乗演算といった処理を行わないために、公開鍵暗号演算を用いる場合と比較して高速に検証のためのデータを生成できることが特徴である。すなわち演算能力の乏しい装置でも検証データを生成できる。また、本方式の処理の流れは、豊富な演算リソースを持たない映像入力装置において簡易な演算による検証データを生成し、次に豊富な演算リソースを有する検証データ変換装置において公開鍵暗号を用いた2次検証データを生成し、検証データを2次検証データに差し替える。最後に映像検証装置では該2次検証データを用いて改竄の検出を行う。このような演算リソースに応じた一連の処理をそれぞれの装置で行うことで、システム全体で安全な改竄検出方法が提供可能となる。

【0063】

豊富な演算リソースを持たない映像入力装置において生成した検証データ（映像データに対して、共有情報との排他的論理和演算を行った後、ハッシュ関数演算を行い、その出力）を用いて映像検証装置において改竄の検出を行うといった方式の場合には、該映像入力装置で使用した共有情報を用いることが必要になるが、該共有情報は2つの装置間のみが知りうる秘密とすることが必須である。もしも該共有情報が改竄者に漏れた場合には、共有情報を用いて検証データを偽造できるので映像データの改竄が可能になる。すなわち、共有情報をどのように2装置間で秘密裏に配送または共有するかという問題がある。

【0064】

一方で、2次検証データを用いて映像検証装置で改竄の検出を行う本方式の場

合には、上記のような共有情報の配送、共有の問題は発生しない。これは、一般の誰にでも公開できる公開情報（公開鍵）を用いて検証を行うためである。

【 0 0 6 5 】

本方式により豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を、秘密に保持する必要がなく、鍵配送の問題がない公開情報（検証データ変換装置で2次検証データを生成する時に使用した秘密情報に対応する情報）を用いるだけで検証可能になった。さらには、該映像データに関するデータを（映像データと）関連付けることでデータベースを作成して管理等を容易にすることができ、トータルな映像データの認証システムを構築することが可能になった。

【 0 0 6 6 】

以下では本実施例における映像入力装置の動作の一例について図9のフローチャートを用いて説明する。

【 0 0 6 7 】

図9は、撮影した映像データに対して共有情報を用いて検証データを生成した後、該検証データを映像データに挿入する処理を説明するためのフローチャートである。

【 0 0 6 8 】

図9において、ステップ91では、被写体の撮影、電気信号処理及びデジタル信号処理、圧縮処理等が行われてフォーマット化された映像データが生成される。

【 0 0 6 9 】

次に、ステップ92では、上記ステップ91で生成された映像データに対して、共有情報との排他的論理和演算を行った後、ハッシュ関数による演算を行い検証データを生成する。

【 0 0 7 0 】

次に、ステップ93では、上記ステップ92で生成された検証データが映像データのヘッダ部に挿入される。

【 0 0 7 1 】

次に、ステップ94では、上記検証データが挿入された映像データに対して送信処理が行われて送出される。該処理は、映像検証装置との間がネットワークで接続されている場合には、該ネットワークにて使用されているプロトコルに応じた変換であり、映像検証装置との間がネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体への記録となる。

【0072】

ここで、1回の撮影毎に、1枚の映像データに対して検証データを生成/挿入する処理をおこなっても良いし、撮影終了後に、撮影した1枚、1枚の各映像データに対して検証データを生成/挿入する処理をまとめて行っても良い。

【0073】

以下では本実施例における検証データ変換装置の動作の一例について図10のフローチャートを用いて説明する。

【0074】

図10は、検証データが挿入された映像データを受信し、映像入力装置と共有する共有情報を用いて映像データの検証および新しい検証データの生成処理を説明するためのフローチャートである。

【0075】

図10において、ステップ101では、検証データが挿入された映像データを映像入力装置から受信する。映像入力装置との間がネットワークで接続されている場合には、ネットワークから該映像データを受信し、映像入力装置との間がネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体経由で受け取る。

【0076】

次に、ステップ102では、ステップ101で受信した映像データのヘッダ部から該映像データに挿入されている検証データを抽出する。

【0077】

次に、ステップ103では、ヘッダ部を削除した映像データから上記ステップ92と同様に、排他的論理和演算とハッシュ関数による演算を行い検証データを

生成する。

【0078】

次に、ステップ104では、ステップ103で生成した検証データとステップ102で抽出した検証データが一致するかが判断され、一致する場合には、ステップ105に進み、一致しない場合にはステップ106に進む。

【0079】

次に、ステップ106では、映像データが改竄されたことを意味するメッセージを出力し動作を終了する。

【0080】

ステップ105では、映像データ（受け取った映像データからヘッダ部を削除したデータ）に対して、ハッシュ関数による演算を行いダイジェストデータを生成し、さらに該ダイジェストデータに対して秘密情報を鍵とする公開鍵暗号演算を行うことで2次検証データを生成する。ここで、使用した秘密情報は、あらかじめ検証データ変換装置に組み込んでおいてもいいし、検証データ変換装置内部で生成して保持してもよい。

【0081】

ステップ107では、生成された2次検証データがステップ93と同様に映像データのヘッダ部に挿入された後、外部装置とのインタフェース部においてデータ変換された後に送出される。

【0082】

以下では本実施例における映像検証装置の動作の一例について図11のフローチャートを用いて説明する。

【0083】

図11は、検証データが挿入された映像データを受信し、検証データ変換装置が2次検証データ生成の際に用いた秘密情報に対応する公開情報を用いて該映像データの検証を説明するためのフローチャートである。

【0084】

図11において、ステップ111では、検証データが挿入された映像データを受信する。ネットワークで接続されている場合には、ネットワークから該映像デ

ータを受信し、ネットワークで接続されておらず、メモリカード等の記憶媒体でデータのやりとりが行われる場合には記憶媒体経由で受け取る。

【 0 0 8 5 】

次に、ステップ 1 1 2 では、検証データ変換装置が検証データ生成の際に用いた秘密情報に対応する公開情報を取得する。秘密情報と公開情報が該検証データ変換装置にて生成された場合には、検証データ変換装置から取得し、あらかじめ秘密情報が検証データ変換装置に組み込まれているような場合には、該秘密情報に対応する公開情報を公開しているサーバ等の装置から取得する。

【 0 0 8 6 】

次にステップ 1 1 3 では、上記ステップ 1 1 1 で受け取った映像データのヘッダ部に存在する 2 次検証データを抽出する。

【 0 0 8 7 】

次にステップ 1 1 4 では、上記ステップ 1 1 3 にて抽出した 2 次検証データに対して、ステップ 1 1 2 にて取得した公開情報を鍵とする公開鍵暗号演算を行いダイジェストデータを生成する。

【 0 0 8 8 】

次にステップ 1 1 5 では、上記ステップ 1 1 1 で受け取った映像データから 2 次検証データを含むヘッダ部を削除し、ヘッダ部を削除した映像データからハッシュ関数による演算を行いダイジェストデータを生成する。

【 0 0 8 9 】

次にステップ 1 1 6 では、上記ステップ 1 1 4 と 1 1 5 で生成したダイジェストデータを比較し、2 つのダイジェストデータが一致する場合には、ステップ 1 1 7 に進み、一致しない場合にはステップ 1 1 8 に進む。

【 0 0 9 0 】

次にステップ 1 1 7 では、ダイジェストデータが一致しなかったことは、映像データに対して改竄が行われたことを意味するので、映像データが改竄されたことを意味するメッセージを出力し動作を終了する。

【 0 0 9 1 】

次にステップ 1 1 8 では、ダイジェストデータが一致したことは、映像データ

に対して改竄が行われていないことを意味するので、映像データが改竄されていないことを意味するメッセージを出力する。

【 0 0 9 2 】

次にステップ 1 1 9 では、改竄の有無、改竄検出に必要となる公開情報の有るか、どの検証データ変換装置から送られてきたものか、登録日時、検証日時等の情報を映像データと関連付けてデータベースを作成して処理を終了する。

【 0 0 9 3 】

本実施例により豊富な演算リソースを持たない映像入力装置の性能を向上させることなく、該映像入力装置にて撮影した映像データの完全性を、秘密に保持する必要のない公開情報を用いるだけで検証可能になった。

【 0 0 9 4 】

上記実施例の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（CPUあるいはMPU）に格納されたプログラムに従って動作させることによって実施したものも、本発明の範疇に含まれる。

【 0 0 9 5 】

この場合、上記ソフトウェアのプログラムコード自体が上述した実施例の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモリカード、ROM等を用いることができる。

【 0 0 9 6 】

なお、上記実施例は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【 0 0 9 7 】

【発明の効果】

以上説明したように本発明によれば、豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することができる。

【図面の簡単な説明】

【図 1】

本発明に係わる実施例における、映像入力装置の構成を示すブロック図である。

【図 2】

本発明に係わる実施例における、検証データ変換装置の構成を示すブロック図である。

【図 3】

本発明に係わる実施例における、映像検証装置の構成を示すブロック図である。

【図 4】

本発明に係わる実施例における、映像データ検証のためのシステムを示す図である。

【図 5】

本発明に係わる実施例における、検証データの生成法の一例を示す図である。

【図 6】

本発明に係わる実施例における、検証データの生成法の一例の詳細を示す図である。

【図 7】

本発明に係わる実施例における、映像データに挿入されるデータの構成例を示す図である。

【図 8】

本発明に係わる実施例における、2次検証データの生成法の1つを示す図である。

【図 9】

本発明に係わる実施例における、映像入力装置の動作を説明するためのフローチャート図である。

【図 1 0】

本発明に係わる実施例における、検証データ変換装置の動作を説明するためのフローチャート図である。

【図 1 1】

本発明に係わる実施例における、映像データ検証装置の動作を説明するためのフローチャート図である。

【符号の説明】

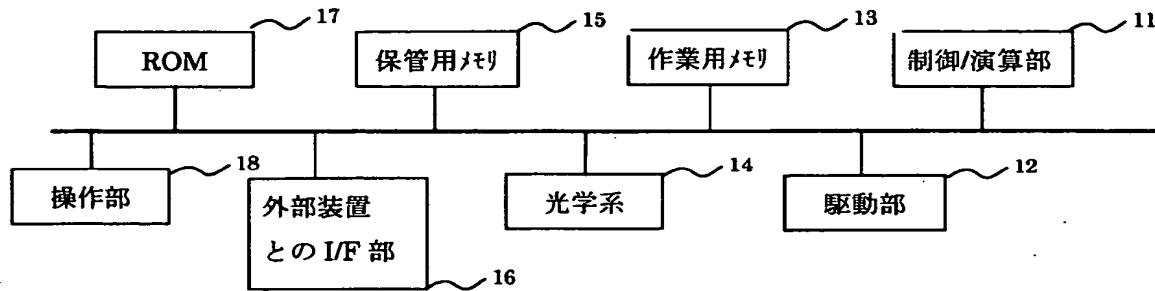
- 1 1 制御／演算部
- 1 2 駆動部
- 1 3 作業用メモリ
- 1 4 光学系
- 1 5 保管用メモリ
- 1 6 インタフェース部
- 1 7 ROM
- 1 8 操作部
- 2 1 制御／演算部
- 2 2 出力部
- 2 3 作業用メモリ
- 2 4 インタフェース部
- 2 5 保管用メモリ
- 2 6 ROM
- 2 7 操作／入力部
- 3 1 制御／演算部
- 3 2 出力部
- 3 3 作業用メモリ
- 3 4 インタフェース部
- 3 5 保管用メモリ

3 6 R O M

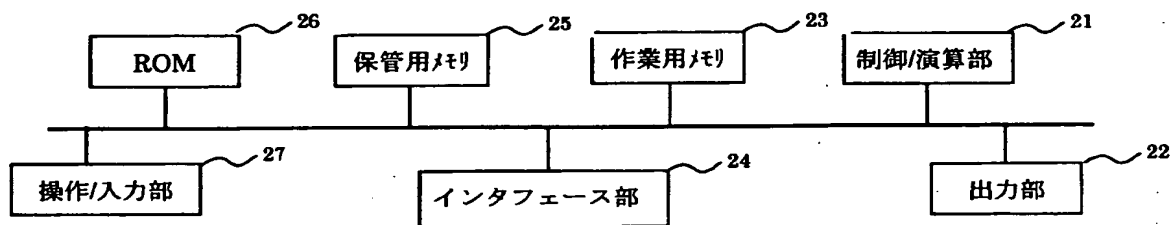
3 7 操 作 / 入 力 部

【書類名】 図面

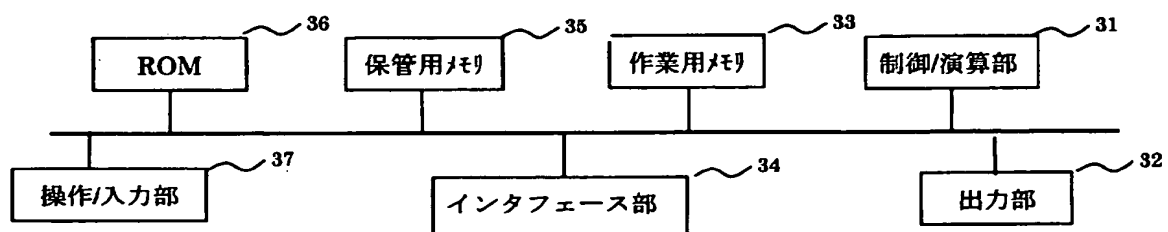
【図 1】



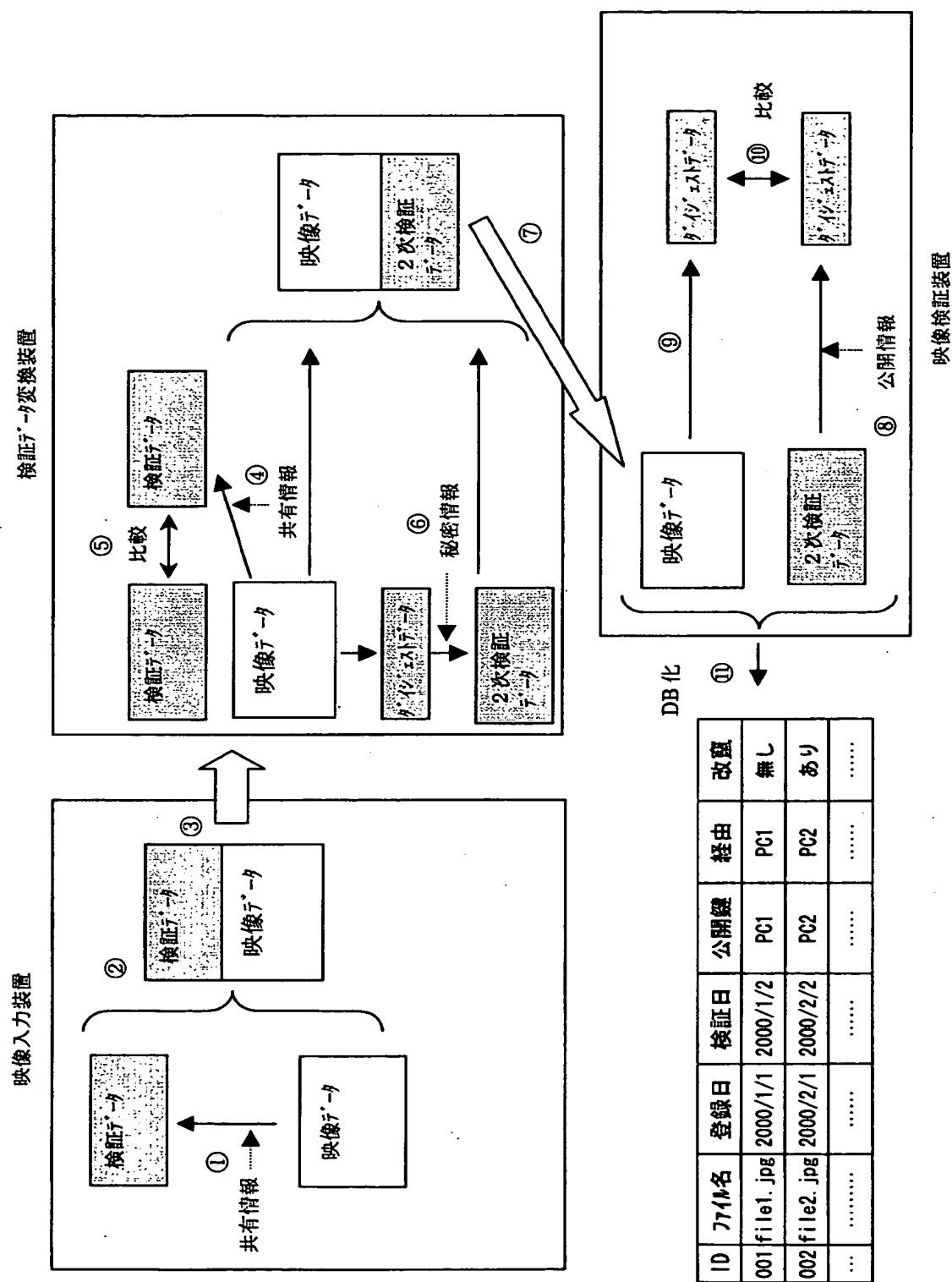
【図 2】



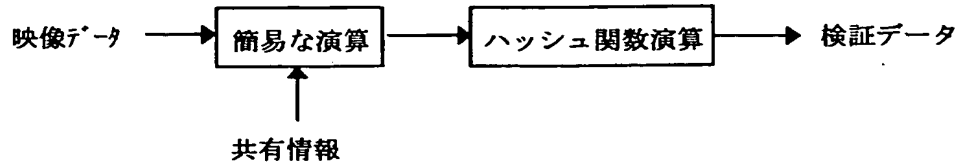
【図 3】



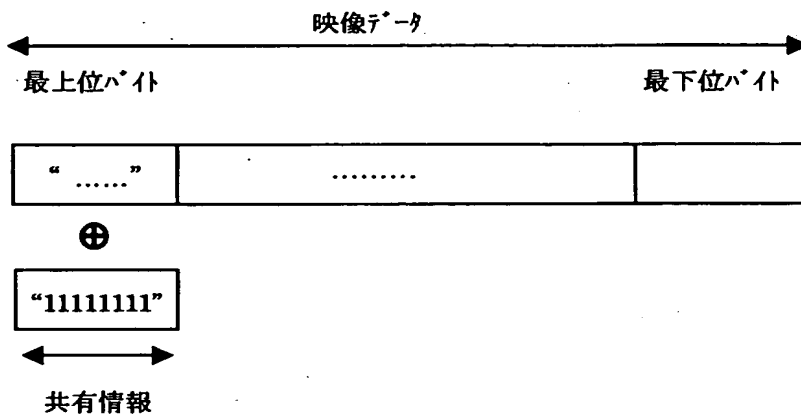
【図 4】



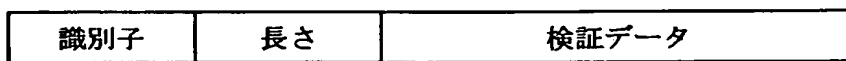
【図 5】



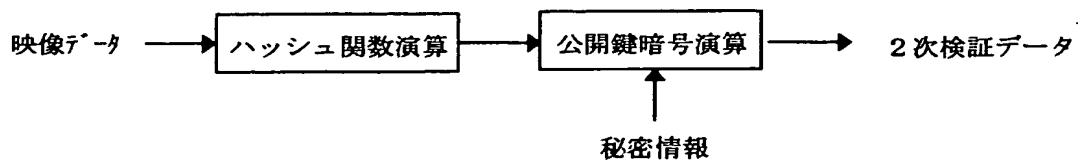
【図 6】



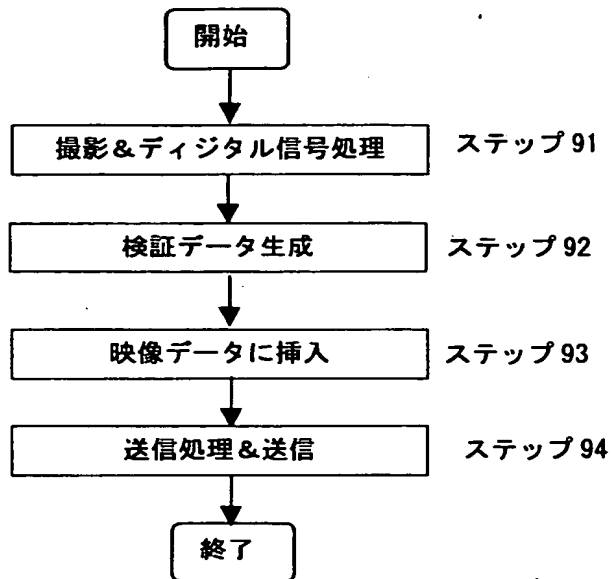
【図 7】



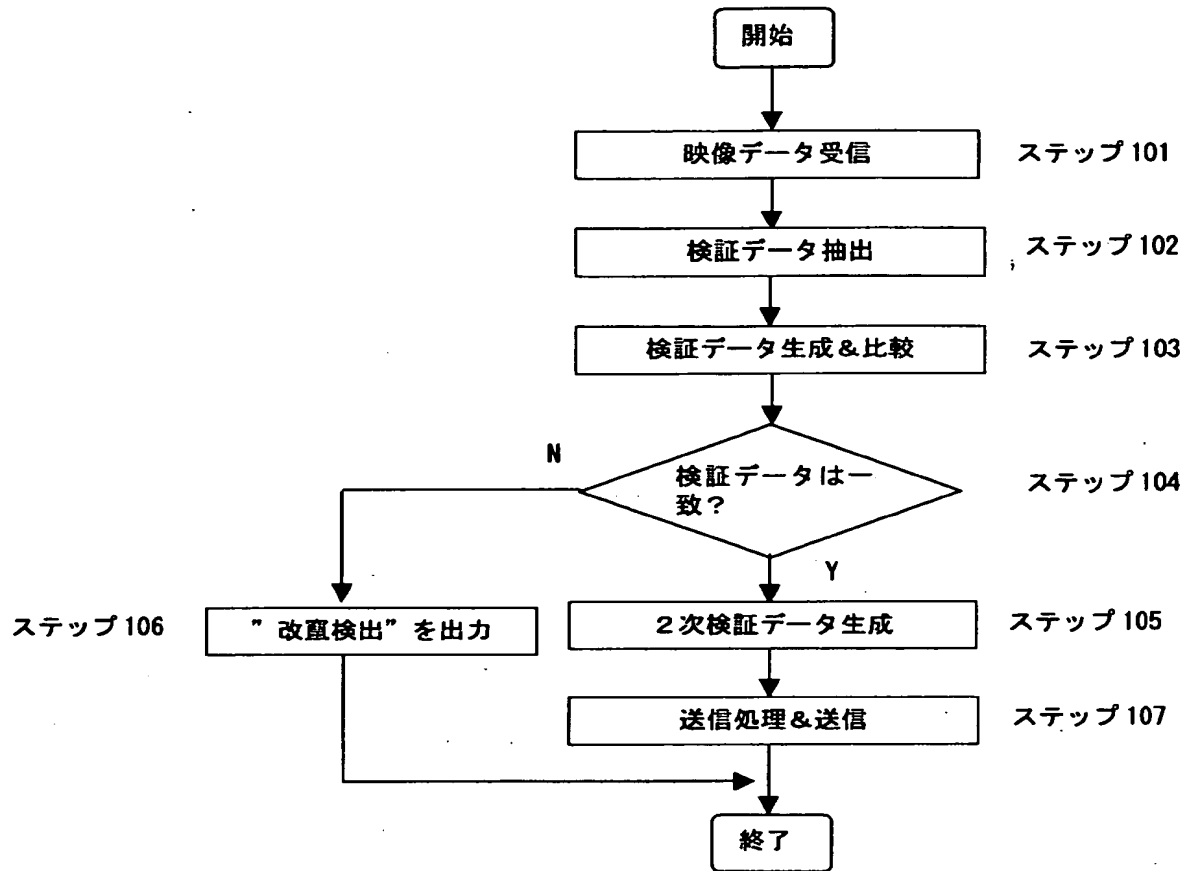
【図 8】



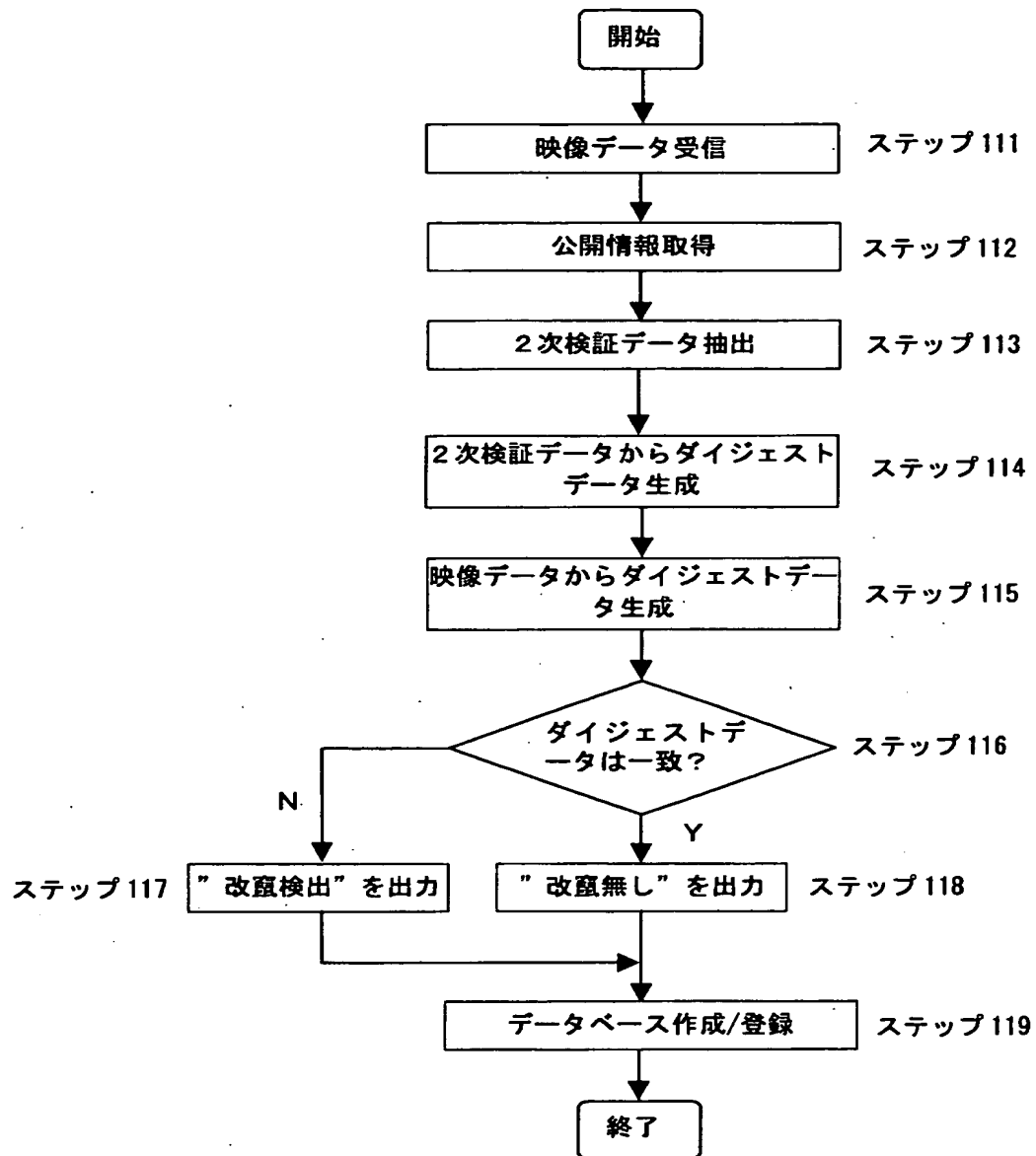
【図 9】



【図 1 0】



【図 11】



【書類名】 要約書

【要約】

【課題】 豊富な演算リソースを持たない映像入力装置の能力を向上させることなく、該映像入力装置にて撮影した映像データの完全性を保証するためのデータを生成することを課題とする。

【解決手段】 本発明の検証データ変換装置は、外部から入力される映像データと、該映像データの検証データと、映像データが生成された装置との間で共有する共有情報とに基づいて該映像データが改竄されていないかどうかを検証する検証処理部と、秘密情報を用いて該映像データから2次検証データを生成する検証データ生成部とを有する。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都大田区下丸子3丁目30番2号
氏 名	キヤノン株式会社